

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3/22/07 has been entered. Any well known art statements made in the last office action that were not adequately and/or specifically traversed are taken as admittance of prior art as per MPEP 2144.03.

Claims 1, 3-11, 13-18, 20-30, 32-35, and 41-47 are pending.

Response to Amendment and Arguments

Applicant's amendment and arguments have been fully considered. Any arguments not specifically addressed below are moot due to new rejections made below.

Note that the rejection of claim 30 is maintained because applicant's arguments for claim 30 were not persuasive. On page 13 of the remarks filed on 3/22/07, applicant argues that claim 30 requires decrypting the first region of the cipher text using the transmitted first encryption key, which differs from Richard's teachings because Richard's KTU cipher text was encrypted using a public key while decrypted using a secret key and the secret key was not transmitted. Applicant argues that because the public key is different from the secret key and the secret key was not transmitted, Richards does not meet the limitations recited in claim 30. The examiner respectfully

Art Unit: 2135

submits that there is nothing recited in claim 30 which requires one to interpret that the same first encryption key was used in both the encryption and decryption of the first region. There is also nothing recited in claim 30 which requires one to interpret that the first encryption key was transmitted to the receiver. Limitations not claimed cannot be considered.

It is noted that the 101 rejection of claim 41 is withdrawn in this office action due to applicant's amendments. The preamble of claim 41 refers to an apparatus implementing a copy protection method. As a person of ordinary skill in the art would understand, software by itself is incapable of performing any action or producing any result until it is functionally tied to some form of hardware. The preamble of claim 41 refers to the apparatus actively performing a task (i.e. implementing a copy protection method), thus implying the apparatus has at least some hardware. It is submitted that claim 41 relies on the preamble for completeness.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claim 1, 4, 5-11, 13-18, 21-30, 32-35, and 41-47 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to

enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Attention is directed to *Sitrick v. Dreamworks* (Fed. Cir 2008). In the cited case, the asserted claims were construed as covering both movies and video games. However, the specification failed to enable use of the claimed invention in movies. Because the full scope of the claim was not enabled, the claims were rejected under 35 USC 112, first paragraph as being non-enabled. The examiner respectfully submits that a similar situation applies to claims 1, 4, 5-11, 13-18, 21-30, 32-35, and 41-47. The full scope of what is being claimed in these claims is not enabled. Claim 1 will be used as a representative claim in this discussion because similar analysis applies to the other claims being rejected under this section.

Claim 1 recites that a first encryption key is used to encrypt a first region of text, the first encryption key is transmitted, and the first region of text is decrypted using the transmitted first encryption key. Note that claims are interpreted in light of the specification. Paragraphs 25-26, 31, and 33 of the specification discloses that the first encryption key is meant to refer to either a symmetric/common key or a public key. Further evidence that the first encryption key can refer to a public key used in a public key encryption method can be seen in the limitation further recited in claim 4 as originally filed, which states that the first encryption key comprises a public key used with a public key encryption method. From these portions of the originally filed disclosure, one sees that the full scope of what is being claimed in claim 1 is such that the first encryption key is either a symmetric key or a public key. However, as a person

Art Unit: 2135

of ordinary skill in the art would understand, in a public key encryption scheme, anything that is encrypted using a public key can only be decrypted using a corresponding private key. It is impossible that a public key be used as a first encryption key to both encrypt and decrypt a first region of text as the full scope of claim 1 is implying. As such, the full scope of claim 1 is not enabled. The examiner had originally assumed that in referring to "a first encryption key" being used in a public key system, applicant meant that "first encryption key" referred to the public/private key pair in a public key system and "first encryption" key could refer to either the public key or the private key. However, as evidenced by remarks filed by applicant on 3/22/07, applicant did not intend for such an interpretation. Because such an interpretation does not apply, it is impossible that a public key be used as a first encryption key for both encryption and decryption of a first region of a text. The full scope of claims 4, 5-11, 13-18, 21-30, 32-35, and 41-47 is such that the first encryption key recited in these claims could also be reasonably interpreted to refer to a public encryption key used for both encryption and decryption, thus the full scope of what is being claimed in these claims also are not fully enabled.

Claim Objections

Claims 30 and 32 are objected to because of the following informalities:

1. As per claim 30, it is respectfully suggested that applicant reorder the steps recited therein in the order that each steps are meant to be carried out. For example, claim 30 recites using the second encryption key to decrypt the second

region before reciting that the first region is decrypted and the second key is extracted for use. One skilled should understand that the second key cannot be used unless the first region is first decrypted and the second key was extracted from the first region.

2. "the second key" in claim 32 should be "the second encryption key".
3. Appropriate correction is required.

Claim Rejections - 35 USC § 102

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim 30 is rejected under 35 U.S.C. 102(e) as being anticipated by Richards (US 6,385,723).

Claim 30:

Richards discloses:

1. Decrypting a first region of the encrypted text using a first encryption key, where the first region contains a second encryption key (col 10, 66-col 11, line 24 and Fig 10, step 1003). *ALU 201 as seen in Figure 2 contains the encrypted application being sent by an application provider and the encrypted security data*

required to protect the application data (col 5, line 66-col 6, line 3). Since the ciphertext AU 201 is formed partially by encrypting the application and security data, the examiner is considering the combination of the non-encrypted application data and the security data as being the claimed text. The ALU 201 seen in Figure 2 is considered the encrypted text. The KTU plain text 601 that is encrypted using mkd_pk (Fig 5, item 507) is considered the claimed first region. KTU plain text as seen in Figure 6 contains key data 615, which the examiner is considering the claimed second encryption key, along with other security data.

2. Decrypting a second region of the encrypted text using the second encryption key (col 11, lines 12-24 and Fig 10, steps 1003-1009). *The key data extracted from the decrypted KTU is used to decrypt AU 203—the second region of the transmitted encrypted text.*
3. Decrypting the first region using region segmentation information (col 10, 66-col 11, line 24 and Fig 10, step 1003). *Key mkd_sk is the reciprocal key of mkd_pk, thus is used to decrypt KTU 207 to retrieve key data 615—the second encryption key. To determine where in the ALU the KTU is located and where in the KTU the key data 615 is located, region segmentation information that was transmitted is utilized.*
4. Extracting the second encryption key from the decrypted first region using information related to the second encryption (col 10, 66-col 11 , line 24 and Fig 10, step 1003).

Claims 34-35 are rejected under 35 U.S.C. 102(e) as being anticipated by Richards (US 6,385,723) as evidenced by applicant's admitted prior art (herein AAPA).

Claim 34:

Richards discloses wherein the size of the second encryption key is varied by a transmission unit within the first region (col 8, lines 57-63 and col 9, lines 12-15). The key length field 613 describes the length of key data 615, i.e. the second encryption key, thus the size of the second encryption key is varied according to field 613.

As per the limitation wherein a size of the first encryption key is fixed, recall that Richards used public key system to secure the first region containing the second encryption key. Keys in a public key system are typically either 512 bit or 1024 bit in size (see as evidence: AAPA, paragraph 3), thus are fixed size. As such, the first encryption key (i.e. mkd_sk) is of fixed size.

Claim 35:

Richards discloses wherein the first region of the encrypted text is smaller than the second region of the encrypted text: As discussed above, the examiner considered the first region of text to be the KTU plain text data, which as seen in Figure 6, contain text data. The examiner considered application data used to create AU 203 (col 6, lines 22-26) as being the second region of text. Application data, i.e. software data, is typically larger than text data, i.e. such as a text file, thus the limitation of the first region of the encrypted text being smaller than the second region of the encrypted text is inherently met by Richards.

As per the limitation that the size of the first encryption key is larger than the size of the second encryption key, Richards also meets the limitation because the first encryption key is a secret key used in a public key system (col 10, line 66-col 11, line 7), which is typically 512 bits or 1024 bits in size (see as evidence: AAPA, paragraph 3) while key data 615 that the examiner is considering the second encryption key is a symmetric key (col 7, lines 17-20), which is 40 bit or 56 bit in size (see as evidence: AAPA, paragraph 3). Because the secret key in a public key system is larger than the private key in the symmetric/common key system, the limitation is met by Richards.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 3, 5-11, 16-17, 13-15, 18, 20, 22-29, 32-33, and 41-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Richards (US 6,385,723) in view of Perlman et al (US 6,912,656) and applicant's admitted prior art (herein referred to as AAPA).

Claim 1:

Richards discloses:

1. Encrypting a first region of a text (i.e. Fig 6, KTU plain text 601) containing a second encryption key (i.e. Fig 6, key data 615) using a public encryption key (Fig 2; Fig 5; Fig 6; col 6, lines 15-26; col 8, lines 40-43; and col 8, line 56-col 9, line 25). *ALU 201 as seen in Figure 2 contains the application being sent by an application provider and the security data required to protect the application data (col 5, line 665-col 6, line 3). Since the ciphertext AU 201 is formed partially by encrypting the application and security data, the examiner is considering the combination of the non-encrypted application data and the security data as being the claimed text. The security data is contained in KTU 207, the plaintext content of which can be seen in Figure 6. The security data as contained in KTU plain text data 601 includes among other items, key data 615, which is considered the claimed second encryption key. The cited portions of Richards shows how the KTU plain text (what the examiner is considering the first region of a text) is encrypted using public key mkd_pk.*
2. Encrypting a second region of the text using the second encryption key (col 6, lines Fig 2, AU 203; Fig 3; col 6, lines 22-26 and 46-46; col 7, lines 15-37). *The application data is encrypted using one or more symmetric keys contained in the KTU to form AU 203. The application data is considered the second region of the text while the data contained in KTU plain text 601 used to encrypt the application data is considered the second encryption key.*
3. Transmitting a cipher text (i.e. Fig 2, ALU 201) comprising the first and second regions (Fig 2; col 10, lines 9-13).

4. Transmitting the region segmentation information for segmenting the text into the first region and the second region, and information related to the second encryption key (Fig 2; col 8, line 57-col 9, line 25; col 10, lines 9-16; col 11, lines 12-21). *The header of the transmitted ALU contains information indicating the starting addresses of AU 203 and KTU 207 and the other components of the ALU. These starting addresses are considered region segmentation information.* The fields in the KTU which describes area start and area length can also be considered region segmentation information since they describe which portions of the application data is encrypted or not encrypted. *The key data field 615 contained in the transmitted KTU contained in the ALU is considered information related to the second encryption key.*
5. Decrypting the first region of the transmitted ciphertext using a secret key (i.e. mkd_sk) and the transmitted region segmentation information (col 10, 66-col 11 , line 24 and Fig 10, step 1003). *Key mkd_sk is the reciprocal key of mkd_pk, thus is used to decrypt KTU 207 to retrieve key data 615—the second encryption key. To determine where in the ALU the KTU is located and where in the KTU the key data 615 is located, region segmentation information that was transmitted is utilized.*
6. Extracting the second decryption key from the decrypted first region using the transmitted information related to the second encryption key (col 10, 66-col 11 , line 24 and Fig 10, step 1003).

7. Decrypting the second region of the transmitted cipher text using the extracted second encryption key (col 11, lines 12-24 and Fig 10, steps 1003-1009). *The key data extracted from the KTU is used to decrypt AU 203--the second region of the transmitted cipher text.*

Richard's invention differs from the invention as recited in claim 1 in that Richard's invention utilizes a public key in the encryption of the text and a secret/private key in the decryption of the first region of cipher text while the invention as recited in claim 1 refers to the encryption and decryption of the first region of text being done using a first encryption key and requires transmitting the first encryption key. Regardless, it would have been obvious to one of ordinary skill in the art at the time applicant's invention was made to modify Richard's invention according to the limitations recited in claim 1 in view of Perlman and AAPA's teachings discussed below.

Perlman shows that at the time applicant's invention was made, both symmetric key systems and asymmetric key systems were known in the art and that it was obvious to use either key system for securing and transmitting key data (Fig 3; col 5, lines 23-63; col 6, lines 56-65; and col 7, lines 4-11). In the cited sections, a message key which was used to encrypt a message sent to a recipient is itself encrypted. The encryption/decryption of the message key could have been done in a number of ways including having the sender use a public key to encrypt the message key while having the recipient use a secret/private key to decrypt the transmitted encrypted message key. Rather than use an asymmetric key system to secure the message key for

transmission, the message key could also have been encrypted and decrypted using the same key as evidenced by use of either a group secret key³¹⁴ or ssl session key 315 to encrypt/decrypt the message key in place of a public/private key pair. The examiner submits that key data 615 of Richard's invention that was encrypted and decrypted using a public/private key pair is equivalent to the message key of Perlman. From Perlman's teachings, it would have been obvious to one of ordinary skill in the art to modify Richard's invention such that rather than use a public/private key pair to encrypt/decrypt the first region of text to secure key data 615, a symmetric key system was used instead such that a first encryption key was used for both the encryption and decryption of the first region containing key data 615.

Further, note from AAPA's discussion of what was known in the art that if a symmetric key was used to encrypt a data, then the symmetric key needs to be securely transmitted to the recipient also since symmetric key systems use the same key for both encryption and decryption of data (Figures 1-2 and paragraph 4-5 and 9-12). From AAPA's teachings, it would have been obvious to one skilled in the art that if one were to modify Richard's invention to use the same first encryption key to both encrypt and decrypt a first region of a text as per Perlman's teachings, then one would also have to transmit the first encryption key to the recipient so that the recipient could decrypt the encrypted first region of text to recover data key 615 of Richards.

The rationale for why it would have been obvious to one of ordinary skill in the art to modify Richard's invention as per Perlman's teachings to use the same first encryption key to both encrypt and decrypt the first region of text is that replacing

Richard's asymmetric key system using Perlman's teachings is simple substitution of one known element for another (i.e. substitute one key-encrypting-key system for another) to obtain predictable results. The rationale for why it would have been obvious to further modify Richard's invention to transmit the first encryption key as per AAPA's teachings is that in symmetric key systems, the same key is used for both encryption and decryption, thus transmitting the first encryption key would ensure that the recipient could decrypt the first region encrypted using the first encryption key.

Claim 3:

Richards, Perlman, and AAPA make obvious all the limitations recited in claim 1. Perlman and AAPA also disclose wherein the first encryption key comprises an encryption key for use with a common key encryption method (Perlman: col 5, lines 60-63; Fig 3, keys 314 and 316; AAPA: paragraph 10).

Claim 5:

The limitation of wherein the second encryption key is smaller than the first encryption key where a common key encryption method is used is obvious to the combination invention of Richards, Perlman, and AAPA. As discussed above, Richard's invention encrypts the first region containing the second/common encryption key using a public key. As recognized by AAPA (paragraph 3), keys used in public key systems are larger than keys used in common key systems and larger keys provide more security, thus a person of ordinary skill in the art having common sense would recognize that Richards used a large key to secure the smaller data key 615 because he wanted a high level of security for the data key. It would have been obvious to one of ordinary

skill in the art to still keep a large sized first encryption key which is larger than the second encryption key even if as per Perlman and AAPA's teachings one were to switch to a common key encryption method to secure the second portion containing the second encryption key. One of ordinary skill would have been motivated to have the second encryption key be smaller than the first encryption key because using a small encryption key for the second encryption key would allow for fast encryption of the application data sent by Richards while using a larger first encryption key would maintain a high level of security for the data key even while switching to a common key system to secure the data key.

Claim 6:

Richards discloses wherein the size of the second encryption key is varied by a transmission unit within the first region (col 8, lines 57-63 and col 9, lines 12-15). The key length field 613 describes the length of key data 615, i.e. the second encryption key, thus the size of the second encryption key is varied according to field 613.

As per the limitation wherein a size of the first encryption key is fixed, recall that Richards used public key system to secure the first region containing the second encryption key. As disclosed by AAPA, public keys are 512 bits or 1024 bits in size, thus are fixed length keys. Large keys provide high level of security, thus even in the combination invention of Richards, Perlman, and AAPA, it would have been obvious to one of ordinary skill in the art having common sense to utilize a key having a large fixed size key as the first encryption key because it would ensure a consistent and high level of security for protecting the first region containing the second encryption key.

Claim 7:

Richards further discloses wherein the information related to the second encryption key includes size and position information of the second encryption key (col 8, lines 57-63 and col 9, lines 12-17). That Richard's invention is able to extract the key data implies that there is information related to the position of where the key data in the KTU plain text.

Claim 8:

As per the limitation of wherein the position and size information of the second encryption key are fixed, official notice is taken that it was well known in the art to fix the position and size information of a key. It would have been obvious to one skilled in the art to further modify Richard's invention such that the position and size information of the second encryption key are fixed because whether the position and size information is fixed or varied is an obvious design choice.

Claim 9:

Richards discloses wherein the position and size information of the second encryption key are varied (col 9, lines 13-15). Note that the size of the key is varied according to the type of encryption technique used. Because the size varies, so too is the position of the second key.

Claim 10:

The limitation of wherein the first region of the text is smaller than the second region of the text is obvious over Richard's teachings. As discussed above, the examiner considered the first region of text to be the KTU plain text data, which as seen

Art Unit: 2135

in Figure 6, contain text data. The examiner considered application data used to create AU 203 (col 6, lines 22-26) as being the second region of text. A person of ordinary skill in the art should appreciate that application data, i.e. software data, is typically larger than text data, i.e. such as a text file, thus the limitation further recited in claim 10 is met by Richards.

Claim 11:

Richards further discloses wherein the region segmentation information comprises information on a starting address of the second region of the text (col 8, line 57-col 9, line 25; col 10, lines 9-16; col 11, lines 12-21).

Claim 16:

Richards further discloses wherein the region segmentation information comprises information on a size of the first region of the text (col 8, line 57-col 9, line 25; col 10, lines 9-16; col 11, lines 12-21).

Claim 17:

The limitation that first encryption key comprises an encryption key that is 56 bit or more is obvious to the combination invention of Richards, Perlman, and AAPA. Recall that as discussed in the rejection of claim 1, it was proposed that Richard's invention be modified by replacing the asymmetric key system used by Richards to encrypt key the first region using a common/symmetric key system instead based on Perlman and AAPA's teachings. Note that AAPA discloses that in the common key encryption method, the key is 56 bit (paragraph 3). As such, in the combination

invention of Richards, Perlman, and AAPA which uses a common key as the first encryption key, the limitation further recited in claim 17 is met.

Claim 13:

Claim 13 is directed towards a copy protection method comprising the decrypting and extracting steps substantially similar to the decrypting and extracting steps recited in claim 1. As such, claim 13 is rejected for substantially similar reasons as discussed in the rejection of claim 1.

Claim 14:

Claim 14 recites a further limitation substantially similar to what is recited in claim 6 and is rejected for similar reasons.

Claim 15:

Claim 15 recites a further limitation that is a combination of what is further recited in claims 5 and 10 and is rejected for similar reasons.

Claim 18:

Claim 18 is directed towards a computer readable medium encoded with processing instructions for implementing a method similar to what is recited in claim 1, thus is rejected for similar reasons as claim 1.

Claim 20:

The limitation that first encryption key comprises a symmetric key having 56 bit or more is obvious to the combination invention of Richards, Perlman, and AAPA. Recall that as discussed in the rejection of claim 1, it was proposed that Richard's invention be modified by replacing the asymmetric key system used by Richards to encrypt key the

first region using a common/symmetric key system instead based on Perlman and AAPA's teachings. Note that AAPA discloses that in the common/symmetric key encryption method, the key is 56 bit (paragraph 3). As such, in the combination invention of Richards, Perlman, and AAPA which uses a common/symmetric key as the first encryption key, the limitation further recited in claim 20 is met.

Claims 22-27:

Claims 22-27 further recite limitations substantially similar to what is recited in claims 5-10 respectively and are rejected for similar reasons as what was discussed in claims 5-10 respectively.

Claim 28:

Richards does not explicitly disclose sending information on a starting address of the second region through a safe transmission path. However, sending information to a receiver about a region's starting address was well known in the art. It was also well known to send information of sensitive nature through a safe or authenticated path. At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify Richard's invention according to the limitations recited in claim 28. One skilled would have been motivated to send information on a starting address of the second region so that the second region could properly be decrypted. One skilled would have been motivated to use a safe transmission path for the sending of information to prevent unauthorized parties from receiving information which could be utilized to decrypt data to which they are not authorized to access.

Claim 29:

Richards discloses sending a cipher text comprising the encrypted first and second regions through an unsafe transmission path (col 10, lines 10-13). AAPA further discloses obtaining the safe transmission path through authentication operations (paragraph 9).

Claim 32:

As per claim 32, Richards does not explicitly disclose wherein the region segmentation information, the information related to the second encryption key, and the first encryption key are received through a safe transmission path. However, official notice is taken that sending confidential information through a safe transmission path was well known in the art at the time applicant's invention was made. Region segmentation information and information related to the second encryption key are utilized to decrypt the encrypted text sent to a receiver, thus can be considered confidential information. As such, it would have been obvious to one of ordinary skill in the art to modify Richard's invention such that region segmentation information and information related to the second encryption key was received by the receiver via a safe/authenticated transmission path. One skilled would have been motivated to modify Richards in the manner discussed because it would prevent unauthorized people from gaining access to confidential information that could be used to decrypt the encrypted text.

As per the limitation that the first encryption key is received through a safe transmission path, note that as discussed in the rejection of claim 1, it would have been obvious to one skilled in the art based on Perlman and AAPA's teachings to modify

Richard's invention such that the first encryption key was a symmetric key such that the first region containing the second encryption key was secured using a symmetric/common key system rather than an asymmetric key system. In this combination invention of Richards, Perlman, and AAPA discussed in the rejection of claim 1, the first encryption key is received through a safe transmission path (AAPA: Figures 1-2 and paragraph 4-5 and 9-12). Because it would have been obvious to one of ordinary skill in the art to modify Richard's invention using Perlman and AAPA's teachings in the manner discussed in claim 1 and for the reasons discussed in claim 1, the limitation that the first encryption key is received through a safe transmission path is obvious to the combination invention of Richards, Perlman, and AAPA.

Claim 33:

Richard further discloses receiving the encrypted text (i.e. ALU 201) through an unsafe transmission path (col 10, lines 10-13).

Claim 41:

Claim 41 is directed towards an apparatus for performing the method of claim 1 and is rejected over the combination teachings of Richards, Perlman, and AAPA for the much the same reason discussed in claim 1. Note that the claimed sender including an authenticator to obtain a safe transmission path is disclosed by AAPA (Fig 1, sender 100 and authenticator 120 and paragraph 4-5 and 9-12). Sender 100 having authenticator 120 performs the transmitting steps recited in claim 1. The claimed encryptor is disclosed by Richards, Perlman, and AAPA (Richards: col 7, lines 15-31 and col 8, lines 40-49; Perlman: col 5, lines 60-63 and Fig 3, item 306; and AAPA: Fig 1,

items 110). The encryptor(s) disclosed by Richards, Perlman, and AAPA are considered to perform the encrypting steps recited in claim 1. Receiver 200 shown in Figure 1 of AAPA includes a decryptor 220 and is considered to perform the extracting and decrypting steps recited in claim 1.

Claim 42:

The limitations further recited in claim 42 are a combination of what is recited in claims 7 and 33 and are rejected for similar reasons.

Claim 43:

Richards does not explicitly disclose the receiver comprises an information appliance. However, official notice is taken that computers being receivers in a cryptographic system was well known in the art at the time applicant's invention was made. Computers are types of information appliances. It would have been obvious to one skilled in the art to modify the combination invention of Richards, Perlman, and AAPA such that the receiver comprised an information appliance. One skilled would have been motivated to do so because cryptography is often used to secure file transfers between computers.

Claim 44:

Richards does not explicitly disclose the receiver comprises a computer. However, official notice is taken that computers being receivers in a cryptographic system was well known in the art at the time applicant's invention was made. It would have been obvious to one skilled in the art to modify the combination invention of Richards, Perlman, and AAPA such that the receiver comprised a computer. One

skilled would have been motivated to do so because cryptography is often used to secure file transfers between computers.

Claim 45:

Richards does not explicitly disclose the receiver comprises a hardware server. However, official notice is taken that receivers being hardware servers was well known in the art at the time applicant's invention was made. It would have been obvious to one skilled in the art to modify the combination invention of Richards, Perlman, and AAPA such that the receiver comprised a hardware server. One skilled would have been motivated to do so because it would allow for secure communication between a client and server.

Claims 46 and 47:

Claims 46 and 47 each recite a method substantially similar to what is recited in claim 1 and are rejected for similar reasons.

Double Patenting

Claims 46 and 47 are objected to under 37 CFR 1.75 as being a substantial duplicate of claim 1. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PONNOREAY PICH whose telephone number is (571)272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Ponnoreay Pich/
Examiner, Art Unit 2135